

## **REMARKS**

Claims 21-22, 24-33, and 35-40 been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,532,218 to Shaffer et al. ("Shaffer") in view of US Patent Publication No. 2004/0117426 to Rudkin and further in view of US Patent No. 7,127,619 to Unger. Claims 21, 32 and 40 are presented in independent form.

Applicants respectfully disagree with the Examiner and traverse the outstanding rejection. Specifically, claims 21, 32, and 40 at the present requires confirmation by the video server of authentication and security authorization information, conveyed by a first encryption technique, entered at the remote computer prior to downloading the video server output signal to each of the remote computers, wherein the transmitted video signal and data signal are encrypted and decrypted via a second encryption technique.

For example, claim 21 discloses a video conferencing system comprising a video server having a specific internet address and a video input port for receiving a source video signal appearing on a video output port of an initiating computer. The video server transforms the source video signal into a video server output signal having a format suitable for communication over the Internet. The system further comprises a plurality of remote computers, where each of the remote computers executes its own respective browser application to allow it to access the video server via the specific Internet address associated with the video server.

The video server downloading the video server output signal to each of the remote computers upon its respective access to the video server, wherein access by the remote computer is verified by a first encryption technique that requires confirmation by the video server of authentication and security authorization information entered at the remote computer and

wherein the video server output signals themselves are encrypted by a second encryption technique,

Further, each of the remote computers decrypts via the second encryption technique and transforms the downloaded video server output signal into a display signal suitable for viewing on a display device associated with that remote computer, and where a representation of the source video signal at the initiating computer is viewable on each of the plurality of remote computers.

As they presently stand, all the independent claims require encryption techniques used both to verify the identity of the remote participant and to encrypt and decrypt the transmitted video and data signals. Specifically, the verification of the user and the encryption of the video and data signals are accomplished using two different encryption techniques. By way of example only, a 128-bit public key RSA encryption technique may be used to verify the information entered by the remote participant at the remote computer, and a 128-bit RC4 private key encryption and decryption technique may be used to encrypt and decrypt the transmitted video signals that are actually sent. Of course other acceptable encryption and decryption techniques are available.

As noted by the Examiner, Schaffer incorporating Rudkin fails to teach or disclose such a configuration or the use of first and second encryption techniques as in the claims. Applicants respectfully disagree with the Examiner's statement that Unger teaches such a system and traverse the present rejection.

The encryption techniques taught in Unger are directed toward encrypting the audio or video content of video conveyed on a cable distribution system for delivering content to numerous types of set top boxes. Assuming *arguendo* that such systems are even related,

Unger does not teach utilizing one encryption technique for verifying that a user is authorized to receive a signal and a separate technique to encrypt the signal. Indeed, Unger does not teach any form of user verification at all. Unger addresses the problem of sending the same signal to numerous set top boxes from different vendors that may all use different proprietary encryption/decryption techniques. Unger is concerned with conserving bandwidth on a cable system and contemplates the use of overlapping encryption techniques to ensure that recipients with different set top boxes (receivers) are all capable of decrypting the received signals regardless of their encryption technology. Unger discloses that several different encryption techniques can be overlaid in the transmission of the audio or video signal and that the clear signals can be shared thereby minimizing the amount of bandwidth required to encrypt signals being sent to various types/technologies of set top boxes.

Unger is silent about utilizing any type of encryption technique to verify that a particular set-top box is authorized to receive the encrypted video signal. Nothing in Unger teaches a system that requires confirmation by a video server (headend) of authentication and security authorization information entered at the remote computer (set top box). In the systems disclosed in Unger, there is no authenticating a user's right to receive a signal as in the present invention. Nothing in Unger teaches or suggests that a set top box user is required to confirm back to the head end, via a signal encrypted using a first technique or otherwise, that it is authorized to receive a signal by entering authentication and security information into the set-top box. Indeed, Unger teaches that it broadcasts all signals to all users regardless of their authority to receive a signal and the respective set top boxes decrypt the signals based on individual encryption technology. In other words, Unger blindly broadcast from the head end, all signals to all users without any affirmative verification that a user is authorized to receive the signal at all. It is only

the set top box's ability to decrypt the general broadcast signal utilizing it's proprietary encryption technique that allows a user to view or listen to the broadcast signal.

Accordingly, Unger fails to teach the use of a video server downloading a video server output signal to each of the remote computers upon its respective access to the video server, wherein access by the remote computer is verified by a first encryption technique that requires confirmation by the video server of authentication and security authorization information entered at the remote computer and wherein the video server output signals themselves are encrypted by a second encryption technique

For at least these reasons, it is believed clear that independent Claim 21 is allowable over Shaffer, Rudkin, and Unger. Independent claims 32 and 40 contain similar limitations as those recited in Claim 21. Accordingly, Applicants submit that Claims 32 and 40 are allowable over the art of record for at least the same reasons set forth above with respect to Claim 21.

The remaining claims all depend from one or another of the independent claims discussed above and are therefore believed patentable for at least the same reasons. Because each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration or reconsideration, as the case maybe, of the patentability of each on its own merits is respectfully requested.

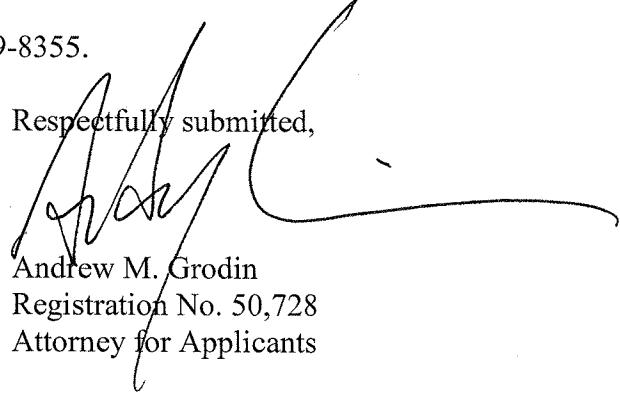
In view of the foregoing amendments and remarks, Applicants respectfully requests favorable reconsideration and allowance of the present application. If, however, there are any unresolved issues, it is requested that the Examiner contact Applicants' representative via telephone so that such issues can be quickly resolved.

*Correspondence and Fees*

Concurrently herewith, Applicants have filed a petition for a three month extension and RCE and the applicable fees. No additional fees are believed to be necessitated by the instant response. However, should a fee be required, authorization is hereby given to charge Deposit Account no. 03-3839 for any underpayment, or to credit any overpayments.

Please address all correspondence to the correspondent address for **Customer No. 26345 of Intellectual Docket Administrator, Gibbons P.C.**, One Gateway Center, Newark, NJ 07102-5310. Telephone calls should be made to Andrew M. Grodin at (973) 596-4553 and fax communications should be sent directly to him at (973) 639-8355.

Respectfully submitted,

  
Andrew M. Grodin  
Registration No. 50,728  
Attorney for Applicants

Gibbons P.C.  
One Gateway Center  
Newark, New Jersey 07102-5310